



King's Research Portal

DOI:

[10.1177/2053951716663965](https://doi.org/10.1177/2053951716663965)

Document Version

Publisher's PDF, also known as Version of record

[Link to publication record in King's Research Portal](#)

Citation for published version (APA):

Birchall, C. (2016). Shareveillance: Subjectivity between open and closed data. *Big Data & Society*, 3(2), 1-12.
<https://doi.org/10.1177/2053951716663965>

Citing this paper

Please note that where the full-text provided on King's Research Portal is the Author Accepted Manuscript or Post-Print version this may differ from the final Published version. If citing, it is advised that you check and use the publisher's definitive version for pagination, volume/issue, and date of publication details. And where the final published version is provided on the Research Portal, if citing you are again advised to check the publisher's website for any subsequent corrections.

General rights

Copyright and moral rights for the publications made accessible in the Research Portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognize and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the Research Portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the Research Portal

Take down policy

If you believe that this document breaches copyright please contact librarypure@kcl.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

Shareveillance: Subjectivity between open and closed data

Clare Birchall

Big Data & Society

July–December 2016: 1–12

© The Author(s) 2016

Reprints and permissions:

sagepub.com/journalsPermissions.nav

DOI: 10.1177/2053951716663965

bds.sagepub.com



Abstract

This article attempts to question modes of sharing and watching to rethink political subjectivity beyond that which is enabled and enforced by the current data regime. It identifies and examines a ‘shareveillant’ subjectivity: a form configured by the sharing and watching that subjects have to withstand *and* enact in the contemporary data assemblage. Looking at government open and closed data as case studies, this article demonstrates how ‘shareveillance’ produces an anti-political role for the public. In describing shareveillance as, after Jacques Rancière, a distribution of the (digital) sensible, this article posits a politico-ethical injunction to cut into the share and flow of data in order to arrange a more enabling assemblage of data and its affects. In order to interrupt shareveillance, this article borrows a concept from Édouard Glissant and his concern with raced otherness to imagine what a ‘right to opacity’ might mean in the digital context. To assert this right is not to endorse the individual subject in her sovereignty and solitude, but rather to imagine a collective political subjectivity and relationality according to the important question of what it means to ‘share well’ beyond the veillant expectations of the state.

Keywords

Sharing, secrecy, opacity, transparency, subjectivity, distribution

Two questions dominate current debates at the intersection of privacy, governance, security, and transparency: How much, and what kind of data should citizens have to *share* with surveillant states? And: How much data from government departments should states *share* with citizens? Yet, these issues are rarely expressed in terms of ‘sharing’ in the way that I will be doing in this article. More often, when thought in tandem with the digital, ‘sharing’ is used in reference to either free trials of software (‘shareware’); the practice of peer-to-peer file sharing; platforms that facilitate the pooling, borrowing, swapping, renting, or selling of resources, skills, and assets that have come to be known as the ‘sharing economy’; or the business of linking and liking on social media, which invites us to share our feelings, preferences, thoughts, interests, photographs, articles, and web links. Sharing in the digital context has been framed as a form of exchange, then, but also communication and distribution (see John, 2013; Wittel, 2011).

In order to understand the politics of open and opaque government data practices, which either share

with citizens or ask citizens to share, I will extend existing commentaries on the distributive qualities of sharing by drawing on Jacques Rancière’s notion of the ‘distribution of the sensible’ (2004a) – a settlement that determines what is visible, audible, sayable, knowable and what share or role we each have within it. In the process, I articulate ‘sharing’ with ‘veillance’ (*veiller* ‘to watch’ is from the Latin *vigilare*, from *vigil*, ‘watchful’) to turn the focus from prevalent ways of understanding digital sharing towards a form of contemporary subjectivity. What I call ‘shareveillance’ – a state in which we are always already sharing; indeed, in which any relationship with data is only made possible through a conditional idea of sharing – produces an

English Department, King’s College London, London, UK

Corresponding author:

Clare Birchall, English Department, King’s College London, Virginia Woolf Building, 22 Kingsway, London WC2B 6LE, UK.

Email: Clare.birchall@kcl.ac.uk



Creative Commons Non Commercial CC-BY-NC: This article is distributed under the terms of the Creative Commons Attribution-NonCommercial 3.0 License (<http://www.creativecommons.org/licenses/by-nc/3.0/>) which permits non-commercial use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

anti-politicised public caught between different data practices.

I will argue that both open and opaque government data initiatives involve, albeit differently pitched, forms of sharing and veillance. Government practices that share data with citizens involve veillance because they call on citizens to monitor and act upon that data – we are envisioned (‘veiled’ and hailed) as auditing and entrepreneurial subjects. Citizens have to monitor the state’s data, that is, or they are expected to innovate with it and make it profitable. Data sharing therefore apports responsibility without power. It watches citizens watching the state, delimiting the ways in which citizens can engage with that data and, therefore, the scope of the political *per se*.

Opaque government data practices (practices that we cannot see through, that are not readily knowable), such as those enacted by the NSA and GCHQ via the PRISM, TEMPORA, and XKeyscore surveillance programs as revealed by Edward Snowden, produce ‘closed’ data. The main point about closed data in relation to the state (and it is important to note at the outset that the details would be different for commercial enterprises) is that it is withheld from general access and circulation for reasons concerned with diplomacy, stability, power play, or security.¹ Despite the sense of restriction, claim, and withholding here, opaque government data practices still involve sharing, however, not least because they require citizens to (often unknowingly) ‘share’ data with the veillant state in a way that renders them visible and trackable.

But we should not think of the positions carved out for citizens in each configuration as an oscillation between agency and impotence. Nor is it quite right to think of this as the ‘equeillance’ diagnosed by Steve Mann (2013) – an evenly poised balance between surveillant and sousveillant forces. Rather, shareveillance constitutes the anti-politicised role the datafied neoliberal security state imagines for its public; the latter is configured more as either a flat dataset or a series of individual auditor–entrepreneurs than as a force with political potential. For those of us unhappy with the political realm being delimited and politics disavowed in this way, we will need to experiment with ways to interrupt shareveillant subjectivity.

A radical critique of ubiquitous and default ‘sharing’ in the digital context is clearly necessary, but I also want to seek out opportunities to salvage this concept in order to imagine a collective political subjectivity that could emerge from within this socio-technical moment (rather than pitching one against it). In this article, then, I will propose that we can interrupt shareveillant subjectivity by claiming not a right to access more data or a right to privacy, but a ‘right to opacity’ (Glissant, 1997). In the context of shareveillance,

I am imagining this right as the demand not to be reduced to, and interact with, data in ways delimited by the state; to resist the terms of engagement set by the two faces of shareveillance (i.e., sharing data with the state and monitoring that shared data). In order to make this argument, I will appropriate the term ‘sharing’ by calling on the etymological roots of ‘to share’ – particularly the Old English for ‘portion’ (*scearu*) which points towards a cutting, shearing, a part, or division. I will posit a right to opacity that cuts into and apart veillant formations and data distributions through various tactics such as hacking, data obfuscation, decentralisation, encryption, anonymity, and anarchic algorithms. Accepting shareveillance means accepting a ‘distribution of the sensible’ that is not based on equality, necessitating a different, more ethical distribution, cut, or share by way of a response on our part. Exploring a right to opacity in the face of shareveillance can politicise the concept of ‘sharing’ by envisioning it as an equitable, ethical cut.

Sharing digitally

Today, sharing with regard to the digital conjures up the range of platforms and apps that facilitate the harnessing of surplus time, skills, goods, and capacities known as the sharing economy. But this is only the latest incarnation of sharing’s articulation within the digital context. Nicholas John (2013) lobbied for sharing to be considered as a keyword for understanding digital culture, in the tradition of Raymond Williams (1976). Subsequently, ‘sharing’ is included in *Culture Digitally’s* ‘Digital Keywords’.² John’s contribution to that project mentions sharing in terms of three examples (2014). First, he calls on computer time-sharing, which was developed during the late 1950s and early 1960s to make efficient use of expensive processor time. Second, John includes file sharing, which informed the U.S. Department of Defense’s development of ARPAnet, and was strengthened by the introduction of Transmission Control Protocol/Internet Protocol (TCP/IP) in 1973 based on the network guiding packets to their destination. Subsequent protocols such as Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol develop the concept that networks can facilitate direct connections and transfers between hosts. Recent peer-to-peer file-sharing techniques present the latest evolution of such logic (see Johnson et al., 2008: 2). Third, John mentions ‘data sharing’ as the term that has, after Snowden, come to denote the simple transportation of data. Though all three of these make an appearance, John chooses to focus on a fourth instance: one embedded in the logic of web 2.0. In this discussion, he turns to the way in which social networking sites have appropriated the

term ‘sharing’ to refer to the imperative and logic of communication and distribution. Because posting, linking, and liking are all termed ‘sharing’ on social networking sites, John claims that, in effect, ‘[s]haring is the fundamental and constitutive activity of Web 2.0’ (2013: 176).

In addition to acting in the service of communication, sharing data also has to be understood as a form of distribution. Human and non-human actors are involved in the dissemination of data, documents, photos, web links, feelings, and news across space and time. Such an obvious point is worth making because it allows us to think beyond the dominant, morally inflected imperative to share or connect with others in a network through a confessional-communicative style, towards circulation in a purely spatial sense (albeit one with ethico-political implications). It might be useful here to think about such a process as one of spatial differentiation – a term borrowed from economics that refers to the uneven dispersal of resources, goods, and services. Differences in natural and human resources lead to inequitable access to inputs and outputs. I want to retain this inflection – of inequality, disparity – with the intention that it will open the way for a broader discussion of the politics or ethics of (data)veillance, distribution, and sharing, in the context of the state rather than private platforms, in the next section.

Distribution of the (digital) sensible

Whereas John’s use of the term ‘distribution’ points towards the act of disseminating photos, files, videos, etc. (2013: 176), I am going to draw on its appearance in the lexicon of Jacques Rancière. Rancière’s *Le Partage du Sensible* is translated as a sharing, partition, division, and, more commonly, distribution of the sensible. This distribution of the sensible is an aesthetico-political settlement. It is, in Rancière’s words:

a delimitation of spaces and times, of the visible and the invisible, of speech and noise, that simultaneously determines the place and the stakes of politics as a form of experience. Politics revolves around what is seen and what can be said about it, around who has the ability to see and the talent to speak, around the properties of spaces and the possibilities of time. (2004a: 12–13)

Aesthetics for Rancière is a distributive regime determining what action, reaction, and thought is possible in any given situation. It is political precisely because in every ‘distribution of the sensible’ equality is either undermined or affirmed. A distribution determines ‘those who have a part in the community of citizens’

(Rancière, 2004a: 7); it ‘reveals who can have a *share* in what is common to the community based on what they do and on the time and space in which this activity is performed [my emphasis]’ (Rancière, 2004a: 8). Equality is enacted when those without part, the unrepresented, come to take part; those without a share, have a share. In a process of subjectivisation,³ this involves refuting the subject position one is allocated by the system, and finding a position, as well as a name or identity-in-relation that will enable full participation and recognition – akin to the work the term ‘proletariat’ once performed (Rancière, 1992). An instantiation of politics based on equality, then, is when demands for a new division and sharing of the social whole are granted.

Such a conception can be helpful in the context of open and opaque government digital data practices, and the shareveillant subjectivity that connects them (which I will come to below). It makes sense today to include digital data in an understanding of the sensible (that which can be seen, heard, touched, thought). Its availability to a subject’s veillant capacities or range, and the conditions of its visibility (to whom, in which circumstances, to what ends) are usefully thought as part of a particular distribution. In any encounter, we can ask: ‘Who has a share of the data?’ and ‘What kind of subjectivity is made more likely as a result of that division and/or access?’ Before turning to discuss these questions in terms of open and opaque government data practices in more detail, I want to pause on the logic of sharing as it pertains to the digital in general, for through this I hope to demonstrate a technological underpinning to the rise of shareveillance.

Sharing as protocological condition

Returning to John’s claim that ‘Sharing is the fundamental and constitutive activity of Web 2.0’ (2013: 176), it is important to note that later, he goes further. ‘It could even be argued that [...] the entire internet is fundamentally a sharing technology’ (179), he writes, citing the importance of open source software and programming languages and sharing economies of production, in the development of websites based on user-generated content. Likewise, Engin Isin and Evelyn Ruppert claim that ‘the ubiquity of various uses of digital trances has made data sharing the norm’ (2015: 89). I want to slightly rephrase and shift the emphasis of John’s assertion to suggest that sharing can be conceived as the constitutive logic of the Internet. Rather than focusing on what users do on the Internet, then, I want to focus more on the idea that sharing operates at a protocological level. My use of this term here draws on Alexander Galloway’s exposition of computer protocols as standards that

‘govern how specific technologies are agreed to, adopted, implemented, and ultimately used by people around the world’ (2004: 7).

This is not intended as a utopian celebration of the Internet’s open, or free, origins. Galloway, among others, makes the error of such an assumption clear, as he characterises the Internet as a technology marked by control and hierarchies of enclosure. Rather, in positing sharing as protocological, I want to imply simply that the Internet’s grain is, first and foremost, ‘stateless’ in the sense that programming intends: as a lack of stored inputs. In other words, the basic architecture of the Internet does not automatically keep a record of previous interactions, and so each interaction request is handled based only on the information that accompanies it. For example, the Internet’s fundamental method for sending data between computers, IP, works by sending small chunks of data, ‘packets’, that travel independently of each other. These discrete packets are put together at an upper layer, by TCP, yet IP itself operates without state. We can also look to how the Web’s HTTP serves up requested pages but does not ‘remember’ those requests. Such discrete communications mean that no continuity is recorded.

As Tom Armitage points out, because the Internet’s default architecture is open or stateless, it is very good at sharing, but not so good at privacy and ownership.⁴ By this, he simply means that ‘implementing state, or privacy, or ownership, or a pay wall, is effort’.⁵ State is a secondary level, patched onto a stateless system. This is categorically not to say that the development and design of the Internet was free from a proprietary impetus, nor that ‘default’ architecture is not conscious and intentional; but rather that to refrain from connecting, and thus in a certain sense, sharing with any network or user at all, at a purely technical level, is something that has to be introduced in secondary layers and mechanisms. It also follows that tracking a user’s activity has to be imposed at a secondary level. Netscape, for example, introduced the cookie – a by-now ubiquitous text file that stores small amounts of data associated with a domain. For as long as the cookie has not expired, it will track the pages a user visits and help build a user profile (see Elmer, 2003). In its stateless formations, before the ‘effort’ to impose statefulness, the Internet, then, can be conceptualised as a technology of stateless, borderless, always already sharing. I want to suggest that sharing (without tracking or remembering) in this instance is a rule conditioning the possibility of computers communicating with each other at all.

However, introducing state, tracking user’s online movements, say, foregrounds a different kind of ‘sharing’ – no longer one concerned with open and non-accumulative peer-to-peer communication,

but rather a ‘sharing’ of the journey, searches, and data transfers from one IP address or an individual user with the web publisher and, often, third parties. Indeed, tech companies like Facebook and Google use the word ‘sharing’ when referring to the monetisation of users’ data (see John, 2013). In Instagram’s 2013 Privacy Policy following its acquisition by Facebook, for example, there is a section entitled ‘Sharing of your Information’.⁶

This links protocol and profits. Illegal and legal entities want a share of our data. This would include hackers should our data be interesting or profitable enough, able to overcome any data loss prevention software and systems from firewalls to encryption. It would also include trackers utilised by web publishers, such as Doubleclick, that log the data we create through our online activity to customise service and advertising and sell it to third parties. Such trackers do not often announce themselves to us unless we seek them out through anti-tracking browser extensions (like Ghostery) or forensic examination of user agreements (which still do not list specific trackers used). Many websites have multiple trackers – cookies and beacons. Ironically, even website publishers that employ trackers are themselves subject to ‘data leakage’ which ‘occurs when a brand, agency or ad tech company collects data about a website’s audience and subsequently uses that data without the initial publisher’s permission’ (McDermott, 2015). Such secretions, the unintentional ‘sharing’ of already ‘shared’ data, also highlight the difficulties of not-sharing from a different perspective.

The idea of sharing as protocological is posited here to emphasise the fact that specific modes of sharing and not-sharing, as well as the particular distribution of the (data) sensible, are determined by ideologically charged *dispositifs*. As Galloway puts it: ‘protocol is how technological control exists after decentralisation’ (2004: 8). Crucially, the conditions of sharing/not sharing today inflect a subjectivity that makes a particular call upon, and imposes a limitation to, the veillant and agential capacities of citizens.

The sharing assemblage

Depending on our politics, we will be more or less resistant to the sharing of our data in exchange for security; depending on our willingness and time to read the clauses in different privacy policies, we might be more or less cognizant of what it is, exactly, we are sharing with private corporations; depending on how much attention we paid to the details of the Snowden revelations, we will have greater or lesser understanding of the ways in which our communications and movements can be monitored by the state. Regardless of the

differentials in knowledge and politics, sharing, I want to argue, has to be understood today not as a conscious and conscientious act but as a key component of contemporary data subjectivity.

Data does not unproblematically belong to us in the first place in order for it then to be 'shared'. Rather, we are within a dynamic sharing assemblage: always already sharing data with human or non-human agents. I want to identify an ascendant shareveillant subjectivity that is shaped by the play between openness and enclosure. 'Shareveillance' is intended to capture the condition of consuming shared data and producing data to be shared in ways that produce a subject who is at once surveillant and surveilled. To phrase it with a slightly different emphasis: the subject of shareveillance is one who simultaneously works with data and on whom the data works.

Sharing prevails as a standard of the system because of the difficulties of un-sharing data and 'effort' of safeguarding or rendering data proprietary. To take the first of these, it is clear that the ease and speed of copying digital data means that data already in circulation cannot be revoked. Moreover, in the case of cloud storage, or even back-ups to hard drives, replication of data is the default. More than one copy of files often exists on a hard drive, let alone in different storage facilities. It is also pertinent to point out that it makes little sense to talk about an 'original' when it comes to digital data, the consequence of which is that data is non-rivalrous and thus sharing non-depleting. We could also look to the way in which the use and re-use of different datasets for various applications makes it nonsensical to talk about the un-sharing of data: once it is the life-blood of various apps, bringing oxygen to a new economy, it is being shared in multiple directions through various media. We can detect, then, a propensity towards duplication, secretion, circulation, and sharing.

While I have pointed towards a distribution of the digital sensible that would encompass private and public, national and transnational entities, for the remainder of this article, I want to focus on the ways in which state forms of 'open' and 'closed' data feed into such a distribution.

Open and closed government data

It is important to note from the outset that the labels 'open' and 'closed' are not essential, but relational, adhering to particular moments in space and time. When articulated to data, the identity of each, and the binary opposition itself, are contingent upon the political climate, the market, the security complex, technological capacities, and the veillant conjuncture. The tendency towards secretion identified above should be enough to indicate the provisional nature of any

identification of data as 'closed'. Likewise, because of the inherently opaque nature of much 'open' data (which leaves many questions unanswered – such as for whom was this data collected? To what ends?), 'open' data is never simply open or transparent.

Open government data is generally understood as the provision of big and small digital data on the part of government agencies. Readers of this journal will know that alongside a few critical voices, open government data is celebrated in the mainstream for democratising knowledge distribution and research, invigorating economies, increasing efficiency, ensuring accountability, and operating as a key element in digital democracy or 'democracy 2.0' (e.g., Goldstein and Dyson, 2013). Open government data is data shared with no depletion: sharing not in the sense of division, but giving multiple citizens access to the same thing.

By contrast, we can understand closed government data as that data which is withheld from public view, whether in the interests of privacy, diplomacy, or national security. As 'close' brings forth etymological associations from the old French *clorre* 'to shut, to cut off from', we can see how citizens are cut off from the state's data, even data they have (perhaps unknowingly) shared. In sharing this kind of data, we have in effect given it away. Our 'share' can never yield. That is to say, without the interventions of whistleblowers or hackers, closed government data will never be given the opportunity to be put to uses other than those determined appropriate by the state.

In its open formation, government data is deliberately and strategically shared by the collecting agent; in its closed formation, data is deliberately and strategically not shared. With respect to closed data, particularly in the case of state surveillance, citizens share data with a proprietary agent in exchange for the privileges that come with citizenship. We might, that is, consciously or unconsciously, explicitly or implicitly consider the collection of our GPS data or phone metadata a fair price to pay for the freedoms, benefits, and protections that come with owning a British (or Australian, German, American, etc.) passport.

This pragmatic attitude to sharing with respect to closed data, the transmission of citizens' activity to a veillant other, is echoed in the experience of digital consumers in general. That is to say, users of social media and search engines are familiar with making trade-offs between services they want and acquiescence to data collection. As well as protocological in a technological sense, then, sharing also needs to be thought as a political, cultural, and industry standard. That is to say, it 'frame[s] the terms and parameters by which elements of a system interact and behave' (McStay, 2014: 5).

As I state above, sharing is not something we do after possessing data, but is the basis on which having

any relation with that data can be possible at all. All of which does not necessarily indicate that the data we have shared is digested and absorbed, and immediately put to work by any surveillant agent. Rather, to borrow the words of Gus Hunt, the CIA's Chief Technology Officer, it indicates that 'collect[ing] everything and hang[ing] on to it forever' (see Ingram, 2013) relies on the idea that the archive is 'structurally speculative' (Andrejevic and Gates, 2014). The uses to which collected data will be put and the meanings it will be given are dependent on future algorithms and political concerns. This means that in a networked era, we are always already sharing without any actor in the system necessarily knowing precisely why. The principle of sharing overrides any uncertainty over the uses to which shared data can be put. Such a condition is obviously in the interests of commercial and state surveillance that, in general, currently have monopolies on accruing economic or security value from big, aggregated archives of data.⁷

While it might seem as though closed government data is open data's evil twin, open government data is not excluded from this veillant assemblage. All shared data mobilises a politics of visibility, a demand to align with a political and ethical distribution of the digital sensible. While the imperative may not be as strong when compared with the dataveillant capacities of the state, open government data initiatives, about which I will provide more detail below, also involve veillance because the sharing of data includes a call to watch and act upon that data – we are envisioned, watched, imagined as entrepreneurial and auditing viewers or subjects. Within a logic of shareveillance, both closed and open data contribute to the construction of an anti-politicised data subject and public. The next section will consider how shareveillant subjectivity is produced in the context of the state rather than commercial practices (though obviously this distinction is undermined by the interdependence between some governments and tech companies as well as the ways those companies can sometimes challenge, exceed, transcend, or evade nation state legislation) by looking at two instantiations: the national security dataveillance revealed by Edward Snowden, and the open government data initiatives implemented by the UK government.

'Closed' data; securitised veillance

The data collected by the NSA, GCHQ, and other security agencies around the globe is mostly experienced as 'closed': inaccessible to those without security clearance. Before Snowden revealed the programs implemented to collect communications data and meta-data – programs such as PRISM, which, since 2007, permitted the NSA to access data from service

providers, and Tempora, which saw GCHQ placing interceptors on fibre-optic cables that handle Internet traffic in and out of the UK – the programs, too, were closed, secret, opaque. That is not to say that there were not all kinds of secretions regarding those practices: details or speculations erupting now and again into the public sphere through reportage, whistleblowing, or popular cultural representation (what Tim Melley refers to as 'the covert sphere' [2012]). Rather than focus on the content of the revelations and whether such news really was new, however, what I am interested in is the conceptual apparatus that was available to those who wanted to resist or challenge this aspect of the shareveillant assemblage.

Though domestic protests were subdued, calls to end the NSA's activities, as evidenced on the banners held at the march on Washington in October 2013, were expressed as an 'end to mass spying'.⁸ Exercising people's imaginations and offending their constitutional rights, was the suggestion that their own government had the ability to see them and their actions without their knowledge or explicit consent. While many would agree that this move towards ubiquitous communications surveillance is, indeed, something to resist, the appeal to 'privacy' falls rather flat. Privacy is like the light we see from an already dead star. We cling to it even though we live in what our digital conjuncture has essentially rendered a post-privacy paradigm. This does not mean that the concept of privacy is no longer important: it still organises legal processes, rights-based debate, and common understandings of our own sense of self. In some ways, as Andy McStay points out:

many social changes since the industrial revolution involve a net increase in privacy, be this less familiarity with our neighbours, more geographically dispersed family arrangements, working away from home, weakening of religious authority [...] greater possibility of children having their own bedrooms, increase in car ownership (versus public transport). (2014: 2)

Yet, the risk of still appealing to privacy in an era of ubiquitous dataveillance and closed, securitised data, is that it reduces rather than increases political agency precisely because it misunderstands the subjectivity in question and because privacy claims are particularly weak when it comes to collective politics. It cannot redistribute the digital sensible.

To take the first of these issues, the appeal to privacy in the wake of the Snowden revelations misreads the de-individualising character of mass covert data mining. The fear expressed on the banners and placards of the poorly attended protests is that the state sees the crowd as individuals; a mass that is made up of many 'I's, the privacy each of which has been infringed. The concept

of privacy imagines a state violating the rights of a fully self-present liberal citizen. But the way in which data mining works means that it is not particularly interested in the actions of individual citizens except in as much as those citizens are data subjects: how they contribute to a background pattern upon which an evolutionary algorithm can work to recognise minority anomalies. As Clough et al. write:

In the case of personal data, it is not the details of that data or a single digital trail that is important, but rather the relationship of the emergent attributes of digital trails en masse that allows for both the broadly sweeping and the particularized modes of affective measure and control. Big data doesn't care about "you" so much as the bits of seemingly random info that bodies generate or that they leave as a data trail... (2014: 154)

Nova Spivack, in an article infused with technoutopianism, puts it slightly differently: 'We are noise, not signal' (2013). While implicitly conflating transparency and surveillance, Spivack invokes this argument to excuse the NSA's data scraping: aligned with the common mantra that if you have done nothing wrong, you have nothing to fear from surveillance. It also points towards our delimited role within the shareveillant assemblage read from the perspective of closed data.

The offence, I suggest, is less the intrusion into personal space and more the anti-political act of only imagining the public as an aggregated dataset. It is not that citizens are being spied on that is of most concern in this view, but that unless their actions are flagged up as extreme outliers, they are not considered fully formed political agents worthy of anything more than bolstering an algorithm for data analysis. Rather than being of comfort, the fact that citizens only count in terms of their role as flat data has an effect on the scope of political agency (even if this is only an imagined agency), and the possibilities therein that this implies for effective, counter-hegemonic collective action. The political is effectively disavowed by shareveillance.

To take the second critique of privacy – that it is a weak foundation on which to build collective action – it is one not tied to the digital/Big Data turn, but it is nevertheless a critique that has been given a new inflection within that context. Privacy has been subject to critique from the Left for its connections with individualism, the perpetuation of oppression, and property. To call on the right to privacy is to frame the debate in terms of an individual's right to limit the access other people, the state, or commercial entities might have to her 'content' (data, thoughts, feelings, information,

communications) at any time. It reinforces a sense of a self that lives in political isolation. Therefore, even when people coalesce around privacy concerns, step into the light of the demos, they do so in order to insist on their right to step back into the apolitical shadows of individualism, away from the possibility of collective creativity or an identity-in-common.

In short, privacy claims are ill-equipped to fundamentally challenge the dataveillance being conducted and its essentially uni-directional sharing of information that contributes to the shareveillant subjectivity I am outlining. But closed data and opaque data practices are only one half of the story.

Open data

The provision of open data is a professed concern and commitment for many liberal democracies today.⁹ The UK's open government data portal, data.gov.uk, is exemplary in this regard, providing public access to many different datasets produced by government agencies.¹⁰ There are many reasons to applaud transparency measures such as this, especially when compared with closed regimes in which extreme forms of corruption are endemic. And yet, this might be an inflammatory comparison, or at least a false construction of the issue. For within ostensibly 'open' liberal democracies, we must ask which forms of openness take precedence in any particular era, and what kind of subjectivities do they produce. Regions wishing to make the move towards more open forms of society and state often look to those *dispositifs* already in operation elsewhere and thus forms of openness, and the political settlements they compound, travel.

In sharing its datasets with citizens, the state adds to the interpellation of shareveillant subjects. 'Hey, you there!' (Althusser, 1971: 174) becomes 'Hey, you there! Come closer and watch'. The subject not only turns to be seen, but also to become vigilant. The shareveillant subject is surveilled (possibly without her knowledge, given all I have said regarding dataveillance), but also has to be seen to be seeing. More accurately, the shareveillant subject is asked to *see through*: the transparency of the state is the interface that hails us and we cannot but occupy the position (whether we feel technically capable or not, whether we perform the function or not) of auditor, analyst, witness. In the process, a characteristic of neoliberal logic is performed: the subject is bequeathed responsibility without power. She is given the responsibility to watch without the expertise to know what to look for, nor the power to act in a meaningful way on what might be found. As Isin and Ruppert recognise, 'acts of sharing place unique demands on citizen subjects of cyberspace' (2015: 88).

The unique demand is not only to look, for even while this call to be vigilant is made, the reach widens to draw in unelected mediators: app developers, data visualisers, etc. Data entrepreneurs step into the ideological call to help fulfil the demand to watch, to see (through) the state. The ‘datapreneurs’ happily perform this function and are also responding to a hailing: to help operationalise the new ‘data economy’. This is because the provision of open government data is fuelled not only by its purported social value, but also its economic value. In an attempt to stimulate and support activity in this economy, governments of developed and developing nations promote and sponsor ‘app-jams’ and ‘datapaloozas’. The ‘datapreneur’ is the key figure in the success of the open data economy, as the actor who must harness the potential of the data to create value from raw datasets. For the state and datapreneur alike, data is configured as a resource ripe for mining and commodification.

Where does this leave the shareveillant subject? At once asked to watch the newly transparent state, with all its data organs on display, and to rely on the mediating and translating functions of a datapreneur to do so, this subject is one whose relationship to government is shaped by the market. Neoliberal ‘capitalist realism’ (Fisher, 2009) has long ensured the public acquiescence to and accommodation of the marketisation of many aspects of social and political life, from education to health. What is new here is that the market gets to decide the very stakes of the political. I am arguing that the reliance upon data mediators or datapreneurs to make the transparency of the state meaningful and legible means that the market decides the distribution of the sensible – what we can know, see, hear, touch, encounter. In terms of sharing, only those government open datasets that can be made to yield profit (in some form) will be translated by datapreneurs in formats that non-specialist citizens can receive, understand, and act upon.

The shareveillant subject is required to be vigilant in order to be an engaged citizen. Immediately, however, this impossible vigilance of the open state is acknowledged, and mediators are called upon to select and package information. This means that vigilance is always watchfulness not of the fully transparent state, but of selected mediations brought forth. Transparency is obscured by its own impossible glare – only the data that the market has primed us to want (usually data that can help us make apparently ‘informed’ choices in a complex public–private landscape) assume the face of state transparency in the data economy. The risk is that it becomes increasingly difficult to participate in and navigate the state outside of these commodified, shaped, and edited forms of aggregated data.

Interrupting shareveillance: New cuts

The shareveillant subject, then, is rendered politically impotent from (at least) two, not necessarily distinct, directions. In the face of state and consumer dataveillance, the subject’s choices (whether that be with whom to communicate or what to buy) are compulsorily shared to contribute to an evolving algorithm to make advertising, say, or governmentality, more efficient, targeted, precise. The public is configured as rich Big Data rather than a network of singularities with resistant potential. Open government portals share the state’s data with subjects and, in doing so, responsabilise and isolate individuals and thus disavow the legitimacy of collective power. In addition, this form of accountability produces a limited relation with the information provided. In monitoring the granular transactions of government – in the form of UK MPs expenses, for example, now available after the scandal of 2009 at www.mpsallowance.parliament.uk – the armchair auditor is only permitted to spot anomalies or aberrations in a system she has to otherwise acknowledge as fair. This form of sharing, of openness, anticipates a limited form of engagement and response. And, as I have outlined above, even this armchair auditor able to engage with ‘raw’ data is largely a fiction produced by the rhetoric of open government; the crucial role that datapreneurs and app developers play in mediating data means that the state’s sharing and the subject’s share of the state are subject to market forces.

I want to be clear that I am not imagining a once fully agential, self-present, sovereign political subject who has now been supplanted by this shareveillant version, compromised by marketised, securitised, and neoliberal apparatus such as algorithmic governmentality and open data portals. Political agency (and presence and sovereignty) has always been limited by structural and relational conditions as well as the fluidity, fragmentation, or fracture of psyches and subjectivities identified by discourses from psychoanalysis to deconstruction. Nevertheless, it is important to recognise the particular discursive-material conditions that curtail political agency – render it beside the point, undesirable, unnecessary – alongside those other inescapable metaphysical limitations. For it is from here that we can more fully understand the particular distribution we are faced with.

It is one thing, of course, to diagnose a condition, and quite another to prescribe a remedy. If one accepts that shareveillance supports a political settlement not conducive to radical equality, and that a more equitable distribution is something to strive for, how might shareveillance be interrupted? I would like to offer one possible strategy, while recognising that there will be others. The conceptual framework for my interruption hinges on the etymology of ‘share’. From the Old

English, *scearu* – ‘a cutting, shearing, tonsure; a part or division’ – the root of the meaning of ‘share’ apropos ‘portion’, to the term *scear*, with respect to plowshare, meaning, simply, ‘that which cuts’, cutting clearly resonates within the concept and practice of sharing. Rather than merely a happy coincidence or useful device, the fact that a cut lies at the heart of sharing attunes us to the ‘violence’ of any distribution.

This focus is certainly supported by Rancière’s framing of the distribution of the sensible, at least in certain translations:

I understand by this phrase the cutting up [decoupage] of the perceptual world that anticipates, through its sensible evidence, the distribution of shares and social parties [...]. And this redistribution itself presupposes a cutting up of what is visible and what is not, of what can be heard and what cannot, of what is noise and what is speech. (Rancière, 2004b: 225)

What share we have of resources, as well as the mode of sharing, fall along the lines of a particular distribution or cut. The way we share, the conditions and decisions underlying how and what we share, what I am calling the ‘cut’, create a certain distribution. As well as the appearance of cutting in the etymology of ‘share’, I am also mindful of Sarah Kember and Joanna Zylinska’s productive use of it in *Life After New Media* (2012). Thinking about mediation as a ‘complex and hybrid process’ that is ‘all-encompassing and indivisible’ (Kember and Zylinska, 2012: xv), the authors draw on a range of thinkers from Henri Bergson to Karen Barad and Jacques Derrida to Emmanuel Levinas, to imagine cuts (into the temporality of mediation) as creative, ethical incisions and decisions. Thus, photography, to take their most potent example, is:

understood here as a process of cutting through the flow of mediation on a number of levels: perceptive, material, technical, and conceptual. The recurrent moment of the cut – one we are familiar with not just via photography but also via film making, sculpture, writing, or, indeed, any other technical practice that involves transforming matter – is posited here as both a technique (an ontological entity encapsulating something that is, or something that is taking place) and an ethical imperative (the command: “Cut!”). (Kember and Zylinska, 2012: xvii–xix)

This leads Kember and Zylinska to ask what it means to ‘cut well’ (2012: xix). It is a question that every artist must ask themselves and practice, they argue. This imperative to cut well extends to all acts of mediation (any other technical practice that involves transforming matter), including the kinds of practices

that mediate data that I engage with in this article. Obviously, not everyone who works with data is an ‘artist’ in the way we would traditionally understand that term. But if we draw on aesthetics in the Rancièrian sense – as a distributive regime that determines political possibilities – then we can begin to see different decisions being made as to how and when to cut into data and what to reveal or conceal about that decision-making process itself, as ethical or unethical.

When we are cut off from our data (as is the case with closed data), we are not given the opportunity to make our own cuts into it. Equally, if the cut of data is such that we can only engage with it in ways that support a political settlement we might not agree with – if what might appear as an ethical provision of data in fact supports or makes more efficient an unethical system – then our cuts are determined with strict parameters. To cut (and therefore share) differently, to cut against the grain, we have to interrupt the strictures of shareveillance.

There are many interruptive cuts I could draw on – hacking, decentralisation, encryption, anonymity – but some of the most interesting can be encapsulated by the term ‘data obfuscation’. Finn Brunton and Helen Nissenbaum (2015: 1) identify a number of different obfuscation strategies that all demonstrate a ‘deliberate addition of ambiguous, confusing, or misleading information to interfere with surveillance and data collection’. In their book, *Obfuscation: A User’s Guide for Privacy and Protest*, Brunton and Nissenbaum consider, among other technologies, the Onion Router (TOR), which allows for online anonymity through a combination of encrypting communication and relaying it via several nodes on the Internet to obscure the source and destination; TrackMeNot, a browser extension that floods search engines with random search terms to render algorithms ineffective; and the privacy plug-in, FaceCloak, which encrypts genuine information offered to Facebook so that it can only be viewed by other friends who also use FaceCloak. Crucially, each interrupts the idea of sharing as the default.

As a particularly decisive cut that utilises obfuscation, I will briefly outline a project published in 2016 by artist Paolo Cirio called ‘Obscurity’.¹¹ In the US, the publication of police photographs, or ‘mugshots’, of arrestees is legal under Freedom of Information and transparency laws in most states. Websites scrape mugshots that have been published elsewhere, sometimes on sites belonging to law enforcement entities, and republish the photographs, requesting money from the arrestee to remove the picture and details. In ‘Obscurity’, Cirio and his collaborators have developed a programme to clone and scramble the data available on mugshot industry websites such as Mugshots.com, Justmugshots.com, and MugshotsOnline.com. Using

almost identical domain names to these sites, Cirio's clone sites show hazy faces that are impossible to identify and names that have been changed. While Cirio is most concerned with the right to be forgotten, as the issue has come to be referred to in the EU after the landmark case in 2014 that ensured search engines like Google are subject to the existing EU data protection directive, we can also read this project as one that exposes the risks inherent to 'sharing' (the risk of abuse and exploitation) and the limits and failures of some transparency initiatives. In addition, with the concerns of the current article in mind, the mugshot industry can be thought of as aping, cynically and darkly, the work undertaken by datapreneurs to transform open data into profitable forms. After all, the websites Cirio is protesting against indeed have an entrepreneurial, creative approach to re-purposing open data.

By cutting into shareveillance, Cirio demands that incarceration be seen not as a decontextualised, individualised problem, but as a collective, social issue for which we all have responsibility. The project exposes the unethical cut of shareveillance with respect to a particular socio-political issue: how, in this case, mugshot websites share data in such a way that presents incarceration as an asocial issue, while in the process performing a second tier of punishment (shaming and extortion) beyond any lawfully imposed penalties. The project asks us to see incarceration in terms of the political economy as well as the stratified and stratifying nature of the carceral state. It cuts into this particular distribution in order to share anew. Creative interruptions of shareveillance can make ethical cuts, and in the process, show up the cuts/incisions that have constructed the neoliberal securitised settlement of which shareveillant subjectivity is a part.

As well as the digital experiments with obfuscation outlined above, cutting into or interrupting shareveillance might include:

- imagining forms of transparency that do not just make already inequitable systems more efficient;
- not using the morally inflected language of sharing when it comes to personal data (see Prainsack, 2015); it is not always 'good' to share;
- insisting on a right to opacity rather than privacy.

In order to help with the last of these, I turn to the late philosopher Édouard Glissant. In a very different context to that with which, this article is engaged, Glissant coined the term a 'right to opacity'. Glissant is writing about an ontological condition of minoritarian subjectivity that resists the demand to be knowable, understood, and transparent in the racialised terms

already set by the dominant group. Unlike privacy, which rests on a subject who, though is knowable in principle, has chosen to keep certain things from view, opacity insists on the irreducible unknowability of the subject. Inspired by this concept, while respecting its origins in work on race, a right to opacity in the digital context would mean the demand not to be reduced to, understood as, consumed, and share data in ways defined by state or consumer shareveillance. Rather than acts of publicity such as legal marches or on-line petitions, I want to argue that we need to meet the pervasive protocols of inequitable dataveillance employed by the securitised state, and the logic of shareveillance with forms of illegibility: a reimagined opacity that allows for a politicality currently denied to subjects to take meaningful forms.

The identity of the shareveilled data object/neoliberal data subject cum dataset is not one that is allowed to interact with data in the creation or exploration of radical collective politics. A right to opacity could be mobilised in order to refuse the shareveillant distribution of the digital sensible. It might offer an opportunity to formulate a politics based not on privacy, but rather, opacity; which could, in turn, clear the way to imagine a community forming openness and exchange rather than its shareveillant manifestation.

It is not a case of deciding whether to accept open data as a compensation for opaque data collection practices and closed data, but of understanding the different ways in which all are part of the shareveillant logic of digital governmentality, and recognising the new epistemological and ontological calls made upon shareveillant subjects.

A right to opacity means, here, the right to refrain from sharing in, and being understood according to a shareveillant distribution we may not support. In this re-attunement, we can reimagine closure as opacity and politicise sharing by understanding it as a series of decisions and cuts. In a conjuncture that places a premium on the knowability and surveillability of subjects, in which everyone must share their data, come forth and be understood as data, these experiments and imaginative cuts become ethical, political acts.

Acknowledgements

I would like to thank the editors of this special volume, the anonymous peer reviewers of *Big Data and Society*, and Gary Hall for their helpful advice on this article.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Notes

1. The UK's Open Data Institute, which works with public and private entities promoting innovation through open data, defines closed data as: 'Data that can only be accessed by its subject, owner or holder' (Broad, 2015).
2. Digital Keywords is a forum hosted by the University of Tulsa, which took inspiration from the 40th anniversary of Raymond Williams' (1976) *Keywords*: <http://culturedigitally.org/digital-keywords/>. The entries are to be published in a forthcoming collection for Princeton University Press (Peters, 2016).
3. See Chambers (2012) on the different incarnations of this term – 'subjectivation' and 'subjectification'.
4. Armitage made these comments during a response he gave at an event centred on James Bridle at The Whitechapel Gallery, 'Systems Literacy', 29 January 2016.
5. Private correspondence with Tom Armitage, 9 February 2016.
6. <https://www.instagram.com/about/legal/privacy/>
7. It is important, of course, to acknowledge that there is also social value to be gained from the sharing of some Big Data, such as genomics data, and other health-related data.
8. See, for example, Reuters' footage at: <http://www.reuters.com/article/us-usa-security-protest-idUSBRE99P0B420131027>
9. The Open Government Partnership currently has 69 participating countries, not all of which, it should be noted, could be described as liberal democracies, at various stages in implementing open government plans: <http://www.opengovpartnership.org/countries>
10. The UK site was launched in 2009, the same year as the US government transparency portal, data.gov. However, the latter's funding was cut in 2011 from \$35 m in 2010 to just \$8 m (Fiveash, 2011).
11. <https://obscurity.online>

References

- Althusser L (1971) Ideology and ideological state apparatuses. In: *Lenin and Philosophy, and Other Essays* (Trans. Brewster B). London: New Left Books, pp.127–188.
- Andrejevic M and Gates K (2014) Big data surveillance: Introduction. *Surveillance and Society* 12(2): 185–196 Available at: <http://library.queensu.ca/ojs/index.php/surveillance-and-society/issue/view/Big%20Data> (accessed 26 July 2016).
- Broad E (2015) Closed, shared, open data: What's in a name? *Open Data Institute Blog*, 17 September. Available at: <https://theodi.org/blog/closed-shared-open-data-whats-in-a-name> (accessed 12 March 2016).
- Brunton F and Nissenbaum H (2015) *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge, MA: MIT Press.
- Chambers SA (2012) *The Lessons of Rancière*. Oxford: Oxford University Press.
- Clough P, Gregory K, Haber B, et al. (2014) The datalogical turn. In: Vannini P (ed.) *Non-representational Methodologies: Re-envisaging Research*. London: Routledge, pp. 146–164.
- Elmer G (2003) *Profiling Machines: Mapping the Personal Information Economy*. Cambridge, MA: MIT Press.
- Fisher M (2009) *Capitalist Realism: Is There No Alternative?* Winchester: Zero Books.
- Fiveash K (2011) Obama's Data.gov CIO quits White House. *The Register*, 16 June. Available at: http://www.theregister.co.uk/2011/06/16/vivek_kundra_quits_cio_job/ (accessed 3 May 2016).
- Galloway A (2004) *Protocol: How Control Exists After Decentralization*. Cambridge, MA: MIT Press.
- Glissant É (1997) *Poetics of Relation* (Trans. Wing B). Ann Arbor, MI: Michigan University Press.
- Goldstein B and Dyson L (eds) (2013) *Beyond Transparency: Open Data and the Future of Civic Innovation*. San Francisco, CA: Code for America Press.
- Ingram M (2013) Even the CIA is struggling to deal with the volume of real-time social data. In: *Gigaom*. 20 March. Available at: <https://gigaom.com/2013/03/20/even-the-cia-is-struggling-to-deal-with-the-volume-of-real-time-social-data/> (accessed 11 April 2016).
- Isin I and Ruppert E (2015) *Being Digital Citizens*. London: Rowman and Littlefield.
- John NA (2013) Sharing and web 2.0: The emergence of a keyword. *New Media and Society* 15(2): 167–182.
- John NA (2014) Sharing. *Digital Keywords*. Available at: <http://culturedigitally.org/2014/05/sharing-draft-digital-keywords/> (accessed 26 July 2016).
- Johnson EM, McGuire D and Willey ND (2008) The evolution of the peer-to-peer file sharing industry and the security risks for users. In: *41st Hawaii international conference on system sciences*, 8–10 January 2008, Waikoloa, Hawaii. Available at: http://digitalstrategies.tuck.dartmouth.edu/cds-uploads/publications/pdf/30750383_1.pdf (accessed 15 February 2016).
- Kember S and Zylinska J (2012) *Life After New Media: Mediation as Vital Process*. Cambridge, MA: MIT Press.
- McDermott J (2015) WTF is data leakage? *Digiday*. January 27. Available at: <http://digiday.com/platforms/what-is-data-leakage/> (accessed 22 January 2016).
- McStay A (2014) *Privacy and Philosophy: New Media and Affective Protocol*. Bern: Peter Lang.
- Mann S (2013) Veillance and reciprocal transparency: Surveillance versus sousveillance, AR glass, lifelogging, and wearable computing. Available at: <http://wearcam.org/veillance/veillance.pdf> (accessed 20 January 2016).
- Melley T (2012) *The Covert Sphere: Secrecy, Fiction, and the National Security State*. Ithaca, NY: Cornell.

- Peters B (ed) (2016) *Digital Keywords: A Vocabulary of Information Society and Culture*. Princeton, NJ: Princeton University Press.
- Prainsack B (2015) Why we should stop talking about data sharing. In: *DNA Digest*. Available at: <http://dnadigest.org/why-we-should-stop-talking-about-data-sharing/> (accessed 5 February 2016).
- Rancière J (1992) Politics, identification, and subjectivization. *October* 61(Summer): 58–64.
- Rancière J (2004a) *The Politics of Aesthetics: Distribution of the Sensible* (Trans. Rockhill G). London: Continuum.
- Rancière J (2004b) *The Philosopher and His Poor* (Trans. Drury J, Oster C and Parker A; Ed. Parker A). Durham, NC: Duke University Press.
- Spivack N (2013) Post-privacy world. *Wired*. Available at: <http://www.wired.com/insights/2013/07/the-post-privacy-world/> (accessed 26 July 2016).
- Williams R (1976) *Keywords: A Vocabulary of Culture and Society*. London: Fontana.
- Wittel A (2011) Qualities of sharing and their transformations in the digital age. *International Review of Information Ethics* 15: 3–8.

This article is a part of Special theme on Veillance and Transparency. To see a full list of all articles in this special theme, please click here: <http://bds.sagepub.com/content/veillance-and-transparency>.